Policy on Evaluating the Effectiveness of Security Policies and Procedures

Introduction

PRECISIONMEDS.COM has adopted this Policy on Determining the Effectiveness of Security Policies and Procedures in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act “ARRA”) and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

PRECISIONMEDS.COM hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information (“IIHI”) generally, and Protected Health Information (“PHI”) as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs periodic Evaluations of the Effectiveness of Security Policies and Procedures for PRECISIONMEDS.COM. All personnel of PRECISIONMEDS.COM must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- PRECISIONMEDS.COM hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- PRECISIONMEDS.COM must comply with HIPAA and the HIPAA implementing regulations pertaining to the periodic evaluation of the effectiveness of security policies and procedures, in accordance with the requirements at § 164.308(a)(8).
- Security policies and procedures, including emergency and contingency plans and procedures, must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

Policy Statement

- It is the Policy of PRECISIONMEDS.COM to periodically evaluate security policies and procedures, including emergency and contingency plans and procedures, in order to improve their effectiveness.
Procedures

- It shall be the responsibility of **Name of Responsible Party or Person** to periodically conduct such technical and nontechnical evaluations.
- **Name of Responsible Party or Person** shall work in coordination with legal counsel, information technology, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
- Such technical and nontechnical evaluations shall be conducted at least every six months (or specify another timeframe).
- The results of such technical and nontechnical evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for emergency preparedness.
- The purpose of such evaluations is to improve the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) that we possess or use.
- **Name of Responsible Party or Person** shall fully document our periodic technical and nontechnical evaluations to determine the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, in accordance with our Documentation Policy and the requirements of HIPAA.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with PRECISIONMEDS.COM’s Sanction Policy.

The material below is for reference purposes only, and does not constitute legal advice.

HIPAA Regulations regarding Evaluations of Security Policies and Procedures, including emergency and contingency plans and procedures...

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
   1.  
      i. **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.
      ii. **Implementation specifications:**
          A. **Risk analysis** (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
B. **Risk management** (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

C. **Sanction policy** (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. **Information system activity review** (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. **Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

3. i. **Standard: Workforce security.** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

   ii. **Implementation specifications:**
      A. **Authorization and/or supervision** (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
      B. **Workforce clearance procedure** (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
      C. **Termination procedures** (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4. i. **Standard: Information access management.** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

   ii. **Implementation specifications:**
      A. **Isolating health care clearinghouse functions** (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
      B. **Access authorization** (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
      C. **Access establishment and modification** (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5. i. **Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).

   ii. **Implementation specifications.** Implement:
B. Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.


6. 
   i. Standard: Security incident procedures. Implement policies and procedures to address security incidents.
   
   ii. Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7. 
   i. Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
   
   ii. Implementation specifications:

   A. Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
   
   B. Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.
   
   C. Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
   
   D. Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.
   
   E. Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

8. Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.

HHS Commentaries regarding Evaluations of Security Policies and Procedures, including Emergency and Contingency Plans and Procedures...

Evaluation (§ 164.308(a)(8))

We proposed that certification would be required and could be performed internally or by an external accrediting agency. We solicited input on appropriate mechanisms to permit an independent assessment of compliance. We were particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf
products used to meet the requirements of this regulation. We also solicited comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.

**HHS Responses to Comments regarding Evaluations of Security Policies and Procedures, including Emergency and Contingency Plans and Procedures...**

**Evaluation (§ 164.308(a)(8))**

*Comment:* We received several comments that certification should be performed externally. A larger group of commenters preferred self-certification. The majority of the comments, however, were to the effect that external certification should be encouraged but not mandated. A number of commenters thought that mandating external certification would create an undue financial burden, regardless of the size of the entity being certified. One commenter stated that external certification would not place an undue burden on a small or rural provider.

*Response:* Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.

*Comment:* Several commenters stated that the certification should cover all components of the proposed rule, not just the information systems.

*Response:* We agree. We have revised this section to reflect that evaluation would be both technical and nontechnical components of security.

*Comment:* A number of commenters expressed a desire for the creation of certification guides or models to complement the rule.

*Response:* We agree that creation of compliance guidelines or models for different business environments would help in the implementation and evaluation of HIPAA security requirements and we encourage professional associations and others to do so. We may develop technical assistance materials, but do not intend to create certification criteria because we do not have the resources to address the large number of different business environments.

*Comment:* Some commenters asked how certification is possible without specifying the level of risk that is permissible.

*Response:* The level of risk that is permissible is specified by § 164.306(a). How such risk is managed will be determined by a covered entity through its security risk analysis and the risk mitigation activities it implements in order to ensure that the level of security required by § 164.306 is provided.

*Comment:* Several commenters requested creation of a list of Federally "certified" security software and off-the-shelf products. Several others stated that this request was not feasible. Regarding certification of off-the-shelf products, one commenter thought this should be encouraged, but not mandated; several thought this would be an impractical endeavor.
Response: While we will not assume the task of certifying software and off-the-shelf products for the reason described above, we have noted with interest that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested (see http://www.niap.nist.gov).

Comment: One commenter stated, "With HCFA's publishing of these HIPAA standards, and their desire to retain the final responsibility for determining violations and imposing penalties of the statute, it also seems appropriate for HCFA to also provide certifying services to ensure security compliance."

Response: In view of the enormous number and variety of covered entities, we believe that evaluation can best be handled through the marketplace, which can develop more usable and targeted evaluation instruments and processes.